



APPENDIX **A**

Administrative Settings User Interface Reference

The following topics describe Security Manager administration settings and related dialog boxes:

- [AutoLink Settings Page, page A-2](#)
- [Configuration Archive Page, page A-3](#)
- [CS-MARS Page, page A-4](#)
- [Customize Desktop Page, page A-7](#)
- [Debug Options Page, page A-7](#)
- [Deployment Page, page A-9](#)
- [Device Communication Page, page A-14](#)
- [Device Groups Page, page A-18](#)
- [Device OS Management Page, page A-19](#)
- [Discovery Page, page A-20](#)
- [IPS Updates Page, page A-22](#)
- [Licensing Page, page A-34](#)
- [Logs Page, page A-39](#)
- [Policy Management Page, page A-40](#)
- [Policy Objects Page, page A-42](#)
- [Rule Expiration Page, page A-43](#)

- [Server Security Page, page A-45](#)
- [Status Page, page A-47](#)
- [Take Over User Session Page, page A-50](#)
- [Token Management Page, page A-51](#)
- [VPN Policy Defaults Page, page A-52](#)
- [Workflow Page, page A-56](#)

AutoLink Settings Page

The Security Manager Map view provides a graphical view of your VPN and Layer 3 network topology. Using device nodes to represent managed devices and map objects to represent unmanaged objects such as devices, clouds, and networks, you can create topology maps with which to study your network. AutoLink settings enable you to exclude any one of five private or reserved networks from Map view. For example, you might want to exclude any test networks that are not relevant to the management tasks you are using Security Manager to perform.

Navigation Path

Click **Tools > Security Manager Administration** and select **AutoLink** from the table of contents.

Related Topics

- [Displaying Layer 3 Links on the Map, page 4-21](#)
- [Displaying Your Network on the Map, page 4-15](#)
- [Understanding Maps, page 4-1](#)
- [Working With Maps, page 4-2](#)

Field Reference

Table A-1 AutoLink Page

Element	Description
Enable AutoLink for 10.0.0.0/8	Whether to automatically include or omit (deselected) these private networks from the maps you create.
Enable AutoLink for 172.16.0.0/12	
Enable AutoLink for 192.168.0.0/16	
Enable AutoLink for 127.0.0.0/8	Whether to automatically include or omit (deselected) the loopback network from the maps you create.
Enable AutoLink for 224.0.0.0/4	Whether to automatically include or omit (deselected) the multicast networks from the maps you create.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Configuration Archive Page

Use the Configuration Archive page to define the default settings for the Configuration Archive tool, including how many configuration versions to save and the TFTP server to use for rolling back Cisco IOS device configurations.

Navigation Path

Click **Tools > Security Manager Administration** and select **Configuration Archive** from the table of contents.

Related Topics

- [Configuration Archive Window, page O-37](#)
- [Rolling Back Configurations, page 19-50](#)

Field Reference

Table A-2 Configuration Archive Page

Element	Description
Max. Versions per Device Purge Now button	The number of configuration versions you want to retain for each managed device, from 1 to 100. If you reduce the number, you can click Purge Now to immediately delete extra versions. Otherwise, Security Manager deletes the extra versions during its normal cleanup cycle.
TFTP Server for Rollback	The fully-qualified DNS host name or IP address of the server to use for TFTP file transfers. TFTP is used during rollback for IOS devices when the configuration cannot be updated using the configure replace command, which does not force a system reload. Enter localhost to use the Security Manager server. By default, a TFTP server is enabled on the Security Manager server. If you specify a remote TFTP server, you must configure that server appropriately to provide TFTP services.
TFTP Root Directory	The root directory for configuration file transfers if you are using the Security Manager server as the TFTP server. Click Browse to select a directory on the Security Manager server. If you specify a server other than the Security Manager server as the TFTP host, Security Manager always uses the root directory of that TFTP server. You cannot specify a non-root directory for remote TFTP servers.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

CS-MARS Page

Use the CS-MARS page to register the Cisco Security Monitoring, Analysis and Response System servers that are monitoring your devices with Security Manager. By registering your CS-MARS servers, you can view syslogs and events captured in CS-MARS based on a device's firewall access rules or IPS signature rules configured in Security Manager. You must register a CS-MARS server before users can see events collected from it.

Navigation Path

Select **Tools > Security Manager Administration** and select **CS-MARS** from the table of contents.

Related Topics

- [Configuring CS-MARS Servers, page 1-25](#)

Field Reference**Table A-3 CS-MARS Page**

Element	Description
CS-MARS Devices	Displays the CS-MARS servers that are registered with Security Manager.
Add button (+ icon)	Click this button to add a server to the list. The New CS-MARS Device dialog box opens (see New or Edit CS-MARS Device Dialog Box, page A-6).
Edit button (pencil icon)	Click this button to edit the properties of the selected server. The Edit CS-MARS Device dialog box opens (see New or Edit CS-MARS Device Dialog Box, page A-6).
Delete button (trash can icon)	Click this button to delete the selected server. When you delete a server, the device properties for all devices that use the server are updated to remove the server connection.
When Launching CS-MARS Allow User to Save Credentials	<p>The type of credentials Security Manager should use to log into CS-MARS when obtaining event information:</p> <ul style="list-style-type: none"> • Prompt users—When the user tries to get event information from CS-MARS, prompt the user to log into CS-MARS. If you select this option, you can also select Allow User to Save Credentials, which gives users the option to save their credentials so they do not have to log into CS-MARS again the next time they request event status. • Use CS-Manager Credentials—When the user tries to get event information from CS-MARS, log into CS-MARS using the same user name and password the user used to log into Security Manager.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.

New or Edit CS-MARS Device Dialog Box

Use the New or Edit CS-MARS Device dialog box to register a CS-MARS server with Security Manager. Users can obtain syslog or event status for a device's firewall or IPS policies from the CS-MARS server that is monitoring the device.

Navigation Path

To open this dialog box, select **Tools > Security Manager Administration**, then click **CS-MARS** to open the CS-MARS page. Then, do one of the following:

- Click the Add button to register a new server.
- Select an existing server and click the Edit button to edit the server properties.

Related Topics

- [Configuring CS-MARS Servers, page 1-25](#)
- [CS-MARS Page, page A-4](#)

Field Reference

Table A-4 Add or Edit CS-MARS Device Dialog Box

Element	Description
CS-MARS Hostname/IP	The IP address or fully-qualified DNS host name of the CS-MARS server.
Username Password	The user name and password for logging into the server to validate that the CS-MARS server is running the appropriate software version and to obtain other basic information. Security Manager also uses this account to determine which CS-MARS server is monitoring a particular device.
Certificate Thumbprint Retrieve From Device button	The CS-MARS server certificate, a hexadecimal string that is unique to the device. Click Retrieve From Device to have Security Manager retrieve the certificate from the CS-MARS server. If the certificate is retrieved successfully, it is displayed. After verifying the certificate, click Accept to save it on the Security Manager server. You must have a correct certificate to use the CS-MARS server from Security Manager.

Customize Desktop Page

Use the Customize Desktop page to control whether Security Manager closes automatically after being idle for a specified time, and to reset whether you are prompted to verify your actions in certain circumstances.

Navigation Path

Select **Tools > Security Manager Administration** and select **Customize Desktop** from the table of contents.

Field Reference

Table A-5 *Customize Desktop Page*

Element	Description
Reset 'Do Not Ask' on Warnings button	Click this button to reestablish 'Are you sure...?' pop-up warnings. When you perform some actions, you are warned about the consequences and you are given the option to not be warned again. If you selected Do Not Ask Me Again for any of these warnings, clicking this button re-enables the warning.
Enable Idle Timeout Idle Timeout (minutes)	Whether to have the Security Manager client close automatically if you do not use it for the specified period of time. If you select this option, enter the number of minutes that must elapse before closing the client in the Idle Timeout field. The default is to close the client after 120 minutes of inactivity.
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Debug Options Page

Use the Debug Options page to configure the severity level of messages to include in debugging logs. You should change debugging levels only if the Cisco Technical Assistance Center (TAC) asks you to change them. This makes it possible for you to include more detailed information in the CSMDiagnostics.zip file.

After you change the message level for the appropriate subcomponent, redo the actions that are resulting in system problems. After the problems occur, create the CSMDiagnostics.zip file by selecting **Tools > Security Manager Diagnostics**. You can then reset the debug options to the default levels so that the Security Manager server does not become bogged down collecting extra debug information. For more information about generating the CSMDiagnostics.zip file, see [Creating a Diagnostics File for the Cisco Technical Assistance Center, page 21-19](#).

By default, logs contain messages of the Error severity or worse. The severity levels in order of severity are:

- Severe—Problems that make the system unusable.
- Error—Problems from which Security Manager cannot recover.
- Warning—Unexpected conditions from which Security Manager can recover.
- Info—Informational messages.
- Debug—Internal status information.

Navigation Path

Select **Tools > Security Manager Administration**, then select **Debug Options** from the table of contents.

Field Reference

Table A-6 *Debug Options Page*

Element	Description
Deployment Debug Level	The message severity level for deployment-related actions such as device communication.
Firewall Services Debug Level	The message severity level for firewall-related policies.
IOS Platform Debug Level	The message severity level for Cisco IOS Software platform policies.
PIX Platform Debug Level	The message severity level for PIX platform policies.
VPN Services Debug Level	The message severity level for VPN services policies.

Table A-6 **Debug Options Page (Continued)**

Save button	Saves your changes.
Reset button	Restores all fields to their previous values.
Restore Defaults button	Resets values to Security Manager defaults.

Deployment Page

Use the Deployment page to define the default methods by which Security Manager deploys configurations to devices. You can override some of these settings when you create deployment jobs.

Navigation Path

Select **Tools > Security Manager Administration** and select **Deployment** from the table of contents.

Related Topics

- [Chapter 19, “Managing Deployment”](#)
- [Chapter 9, “Managing Objects”](#)
- [Chapter F, “Policy Object Manager User Interface Reference”](#)

Field Reference

Table A-7 Deployment Page

Element	Description
Deployment	
Purge Debugging Files Older Than (days)	The maximum number of days the system should keep debugging files. Debug files are automatically deleted. If you decrease the number of days, you can click Purge Now to immediately delete all debugging files older than the number of days specified.
Default Deployment Method Directory	<p>The method to use as the default method for deploying configurations to devices:</p> <ul style="list-style-type: none"> • Device—Deploys the configuration directly to the device or to the transport mechanism specified for the device. For more information, see Deploying to a Device, page 19-11. • File—Deploys the configuration file to a directory on the Security Manager server. If you select File, specify the directory to which you want to deploy the configuration file in the Destination column. For more information, see Deploying to a File, page 19-14. <p>You can override this method when you create deployment jobs.</p>
When Out of Band Changes Detected	<p>How Security Manager should respond when it detects that changes were made directly on the device CLI since a configuration was last deployed to the device. This setting specifies the default action, which you can override when you create deployment jobs. You can choose one of the following:</p> <ul style="list-style-type: none"> • Warn (default)—If changes were made to the device manually, Security Manager continues with the deployment, overwrites the changes, and displays a warning notifying you of this action. • Cancel—If changes were made to the device manually, Security Manager cancels the deployment and displays a warning notifying you of this action. • Skip—Security Manager does not check for changes and deploys the changes to the device, overwriting any local modifications.

Table A-7 **Deployment Page (Continued)**

Deploy to File Reference Configuration	<p>The configuration that Security Manager uses to compare new policies against the previous configuration for the device, if you are deploying the configuration to a file on the Security Manager server.</p> <ul style="list-style-type: none"> • Archive (default)—The most recently archived configuration. • Device—The current running device configuration, which is obtained from the device. <p>After comparing the configurations, Security Manager generates the correct CLI for deployment.</p>
Deploy to Device Reference Configuration	<p>The configuration that Security Manager uses to compare new policies against the previous configuration for the device, if you are deploying the configuration directly to the device (or to a transport server).</p> <ul style="list-style-type: none"> • Archive—The most recently archived configuration. • Device (default)—The current running device configuration, which is obtained from the device. <p>After comparing the configurations, Security Manager generates the correct CLI for deployment.</p>
Optimize the Deployment of Access Rules For	<p>How firewall rules are deployed. You can choose one of the following:</p> <ul style="list-style-type: none"> • Speed (default)—Increases deployment speed by sending only the delta (difference) between the new and old ACLs. This is the recommended option. By making use of ACL line numbers, this approach selectively adds, updates, or deletes ACEs at specific positions and avoids resending the entire ACL. Because the ACL being edited is still in use, there is a small chance that some traffic might be handled incorrectly between the time an ACE is removed and the time that it is added to a new position. The ACL line number feature is supported by most Cisco IOS, PIX and ASA versions, and became available in FWSM from FWSM 3.1(1). • Traffic—This approach switches ACLs seamlessly and avoids traffic interruption. However, deployment takes longer and uses more device memory before the temporary ACLs are deleted. First, a temporary copy is made of the ACL that is intended for deployment. This temporary ACL binds to the target interface. Then the old ACL is recreated with its original name but with the content of the new ACL. It also binds to the target interface. At this point, the temporary ACL is deleted.

Table A-7 **Deployment Page (Continued)**


Firewall Access-List Names	<p>How ACL names are deployed to devices if the access rule does not have a name in Security Manager.</p> <ul style="list-style-type: none"> • Reuse existing names—Reuse the ACL name that is configured in the reference configuration (which is usually from the device). See Preserving User-Defined ACL Names, page 13-59. • Reset to CS-Manager generated names—Reset the name to a Security Manager auto-generated ACL name. See How ACL Names Are Generated, page 13-57.
Let FWSM Decide When to Compile Access Lists	<p>Whether to have the Firewall Services Module (FWSM) automatically determine when to compile access lists. Selecting this option might increase deployment speed but traffic might be disrupted and the system might become incapable of reporting ACL compilation error messages.</p> <p>When deselected, Security Manager controls ACL compilation to avoid traffic interruption and to minimize peak memory usage on the device. For more information, see Understanding Access Rules, page 13-53.</p> <p> Caution You should not select this option unless you are experiencing deployment problems and you are an advanced user.</p>
Enable Advanced Debugging	<p>Whether Security Manager generates data files about configuration generation, deployment, and discovery as these functions are performed. The temporary data files are stored in the MDC\temp directory in the Security Manager installation folder on the server, and you can use these files for debugging purposes.</p> <p>Note Selecting this check box slows down Security Manager response time. Enable debugging only in limited circumstances.</p>
Allow Download on Error	<p>Whether deployments to devices should continue even if there are minor device configuration errors.</p>
Remove Unreferenced Object Groups from Device (PIX, ASA, FWSM)	<p>Whether Security Manager should remove object groups that are not being used by other CLI commands from devices during deployment.</p>

Table A-7 Deployment Page (Continued)

<p>Create Object Groups for Policy Objects (PIX, ASA, FWSM)</p> <p>Create Object Groups for Multiple Sources, Destinations or Services in a Rule (PIX, ASA, FWSM)</p> <p>Optimize Network Object Groups During Deployment (PIX, ASA, FWSM)</p>	<p>Whether Security Manager should create object groups, such as network objects and service objects, to replace comma-separated values in a rule table cell for PIX, ASA, and FWSM devices. When deselected, Security Manager flattens the object groups to display the IP addresses, sources and destinations, ports, and protocols for these devices.</p> <p>If you select this option, you can also select these options:</p> <ul style="list-style-type: none"> • Create Object Groups for Multiple Sources, Destinations or Services in a Rule (PIX, ASA, FWSM)—Whether to automatically create network objects and service objects to replace comma-separated values in a rule table cell that resulted when multiple rules were combined. The objects are created during deployment. For more information, see Combining Rules, page 13-12. • Optimize Network Object Groups During Deployment (PIX, ASA, FWSM)—Whether to optimize network object groups by making them more succinct. For more information on optimizing policy objects, see Optimizing Policy Objects in Rules, page 13-51.
<p>Remove Unreferenced Access-lists on Device</p>	<p>Whether to delete any access lists that are not being used by other CLI commands from devices during deployment.</p>
<p>Save Changes Permanently on Device</p>	<p>Whether to save the running configuration to the startup configuration (using the write memory command) after deploying a configuration to a device. This applies to PIX, FWSM, ASA, or Cisco IOS devices. If you deselect this check box, the startup configuration is not changed, which means your configuration changes will be lost if the device reloads for any reason.</p>
<p>Generate ACL Remarks During Deployment</p>	<p>Whether to display ACL warning messages and remarks during deployment.</p>
<p>Preselect Devices with Undeployed Changes</p>	<p>Whether the list of changed devices you see when you create a deployment job has all changed devices preselected. If you deselect this option, users must manually select the devices to include in the deployment job.</p>
<p>Enable Auto Refresh in Deployment Main Panel</p>	<p>Whether the deployment job and schedule status information should be automatically refreshed in the Deployment Manager window. If you deselect this option, you must click the Refresh button to refresh the information manually.</p>
<p>Save button</p>	<p>Saves and applies changes.</p>

Table A-7 **Deployment Page (Continued)**

Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Device Communication Page

Use the Device Communication page to define default settings for communicating with devices. These settings mainly affect device inventory and policy discovery and configuration deployment. You can override the transport settings for individual devices in the device properties for the device.

If you change the transport protocol settings, ensure that your devices are appropriately configured to accept those types of connections.

Navigation Path

Select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents.

Related Topics

- [Adding Devices to the Device Inventory, page 6-8](#)
- [Chapter 6, “Managing the Device Inventory”](#)
- [Chapter 5, “Preparing Devices for Management”](#)
- [Viewing or Changing Device Properties, page 6-23](#)

Field Reference

Table A-8 **Device Communication Page**

Element	Description
Device Connection Parameters	
Device Connection Timeout	The number of seconds that Security Manager has to establish a connection with a device before timing out.
Retry Count	The number of times that Security Manager should try to establish a connection to a device before concluding that the connection cannot be completed. The default value is 3.

Table A-8 Device Communication Page (Continued)

Socket Read Timeout	For SSH and Telnet sessions, the maximum number of seconds Security Manager can wait for incoming data before concluding that the connection is lost.
Transport Protocol (IPS)	The default transport protocol for IPS sensors and routers that include the IPS feature. The default is HTTPS.
Transport Protocol (IOS Routers 12.3 and above)	The default transport protocol for routers that run Cisco IOS software release 12.3 and above. The default is HTTPS.
Transport Protocol (Catalyst Switch/7600)	The default transport protocol for Catalyst 6500/7600 devices and all other Catalyst switches, regardless of the Cisco IOS software version running on the devices. The default is SSH.
Transport Protocol (IOS Routers 12.2, 12.1)	The default transport protocol for routers that run Cisco IOS software releases 12.1 and 12.2. The default is Telnet.
Connect to Device Using	<p>The type of credentials Security Manager should use when accessing devices. For more information, see Understanding Device Credentials, page 6-4.</p> <ul style="list-style-type: none"> • Security Manager User Login Credentials—Security Manager contacts the device using the credentials that you entered while logging in to Security Manager. The same set of credentials are used for all devices regardless of the credentials configured for each device on the Device Credentials page. • Security Manager Device Credentials—Security Manager contacts the device using the credentials specified in the Device Properties Credentials page. This is the default.

Table A-8 Device Communication Page (Continued)

SSL Certificate Parameters	
Device Authentication Certificates (IPS) Device Authentication Certificates (Router) PIX/ ASA/ FWSM Device Authentication Certificates Add Certificate button	<p>How to handle device authentication certificates for SSL (HTTPS) communications. You can configure different behaviors for different types of devices, but the settings have the same meaning:</p> <ul style="list-style-type: none"> • Retrieve while adding devices—Security Manager automatically obtains certificates from the devices while you add devices from the network or from an export file. • Manually add certificates—Security Manager does not automatically accept certificates from the device. Click Add Certificate to open the Add Certificate dialog box (see Add Certificate Dialog Box, page A-18) where you can manually add the thumbprint before you try to add the device from the network or from an export file. You can also add certificates for devices that you create manually from the Device Properties Credentials page to be successful. For more information, see Manually Adding SSL Certificates for Devices that Use HTTPS Communications, page 6-25. • Do not use certificate authentication—Security Manager ignores device authentication certificates. This option leaves your system vulnerable to third-party interference with device validation. We recommend that you do not use this option.
Accept Device SSL Certificate after Rollback	For devices that use SSL, whether to obtain the certificate installed on an IPS device, firewall device, FWSM, ASA, or Cisco IOS router from the device when you roll back the configuration on the device.

Table A-8 Device Communication Page (Continued)

HTTPS Port Number	<p>The default port number that the device uses for secure communication with Security Manager (as well as other management applications that use these protocols). This value overrides the HTTPS port number that you configure in the HTTP policy for a device.</p> <p>Note If you configure the local HTTP policy to be a shared policy and assign the HTTP policy to multiple devices, the HTTPS port number setting in the shared policy overrides the port number configured in the Device Properties Credentials page for all devices to which the policy is assigned.</p> <p>In addition to providing access to the device through the Cisco web browser user interface, the HTTPS port number is used by device management applications, such as the Cisco Router and Security Device Manager (SDM), and monitoring tools, such as IPS Event Viewer (IEV), to communicate with the device.</p> <p>Note The security appliance can support both SSL VPN connections and HTTPS connections for device manager administrative sessions simultaneously on the same interface. Both HTTPS and SSL VPN use port 443 by default. Therefore, to enable both HTTPS and SSL VPN on the same interface, you must specify a different port number for either HTTPS or WebVPN. An alternative is to configure SSL VPN and HTTPS on different interfaces.</p>
Overwrite SSH Keys	<p>Whether Security Manager can overwrite the SSH key for a device when it changes on the device. For SSH connections, a correct key is required for successful communication.</p> <p>Deselect this check box with caution, and only if you require a greater level of security. Security Manager does not communicate with the device if keys are changed on the device.</p>
Save button	Saves and applies changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Add Certificate Dialog Box

Use the Add Certificate dialog box to add device certificates manually for devices that use the SSL transport protocol (firewall devices, FWSMs, ASAs, IPS devices, and Cisco IOS devices). Adding the device certificates manually gives you the highest level of security because then an intruder is prevented from introducing a fraudulent certificate thumbprint. Device certificates are stored in the database to be used for device authentication.

For more information about manually adding SSL certificates, see [Manually Adding SSL Certificates for Devices that Use HTTPS Communications](#), page 6-25.

Navigation Path

Select **Tools > Security Manager Administration**, select **Device Communication** from the table of content, and click **Add Certificate**.

Field Reference

Table A-9 *Add Certificate Dialog Box*

Element	Description
Host Name or IP Address	The hostname or IP address of the device for which you are adding the certificate.
Certificate Thumbprint	The certificate thumbprint, which is a string of hexadecimal digits that is unique to the device.

Device Groups Page

Use the Device Groups page to manage the device groups and group types defined in the device inventory.

Navigation Path

Select **Tools > Security Manager Administration**, then select **Device Groups** from the table of contents.

Related Topics

- [Understanding Device Grouping, page 6-36](#)
- [Working with Device Groups, page 6-36](#)

Field Reference**Table A-10** **Device Groups Page**

Element	Description
Groups	Displays the device groups and group types. To rename a group or type, select it and then click it again to make the text editable. Type in the new name and press Enter.
Add Type button	Click this button to create a new group type. The type is added with a default name. Overtyping the name and pressing Enter.
Add Group to Type button	Click this button to add a device group to the selected device group or group type.
Delete button (trash can)	Click this button to delete the selected device group or group type and all device groups that it contains. Deleting a device group or group type does not delete any devices it contains.
Save button	Saves your changes.
Reset button	Restores all fields to their previous values.

Device OS Management Page

Security Manager includes shortcut commands to access several key features of Resource Manager Essentials (RME). To enable these commands, you must identify the RME server to Security Manager on this page.

Navigation Path

Select **Tools > Security Manager Administration** and select **Device OS Management** from the table of contents.

Related Topics

- [Resource Manager Essentials Documentation](#)
- [Managing the Device Operating System, page 6-35](#)

Field Reference

Table A-11 Device OS Management

Element	Description
RME server address	The IP address or fully-qualified hostname of the RME server.
Connect using https	Whether to connect to the RME server using SSL.
Save button	Saves your changes.
Reset button	Restores all fields to their previous values.
Restore Defaults button	Resets values to Security Manager defaults.

Discovery Page

Use the Discovery page to define how Security Manager should handle certain types of objects or events during inventory and policy discovery. You can also control how long Security Manager keeps discovery tasks.

Navigation Path

Select **Tools > Security Manager Administration** and select **Discovery** from the table of contents.

Related Topics

- [Understanding Policies, page 7-1](#)
- [Discovering Policies, page 7-7](#)
- [Understanding the Policy Object Manager Window, page 9-5](#)

Field Reference

Table A-12 Discovery Page

Element	Description
Prepend Device Name when Generating Security Context Names	<p>Whether the name of the device that contains the security context should be added to the front of the security context's name. For example, if a security context is named admin, and it is contained in the device with the display name 10.100.15.16, the name that will appear in the Device selector is 10.100.15.16_admin.</p> <p>If you do not prepend the device name, the security context name appears in the inventory by itself. Because Security Manager does not place security contexts in a folder related to the parent device, the only way to easily see contexts that are related to a device is to prepend the device name.</p> <p>If you do not prepend device names, Security Manager adds a numbered suffix to distinguish identically named devices. For example, if the admin context exists in more than one firewall, you will see admin_01, admin_02, and so on, in the Device selector.</p>
Purge Discovery Tasks Older Than	The number of days to save discovery and device-import tasks. Tasks older than the number of days you enter are deleted.
Reuse Policy Objects for Inline Values	Whether to substitute any named policy objects, such as IP addresses already defined in Security Manager, for inline values in the CLI. For more information on policy objects, see Chapter 9, "Managing Objects" .
Allow Device Override for Discovered Policy Objects	For certain types of objects, whether to allow users to override the parent object values at the device level for policy objects that are discovered. For more information, see Overriding Global Objects for Individual Devices, page 9-214 .
On Error, Rollback Discovery for Entire Device	Whether Security Manager should roll back all discovered policies if even one error is encountered for a single policy during policy discovery. When deselected, Security Manager keeps the policies successfully discovered and discards only those policies with errors. For more information on policy discovery, see Discovering Policies, page 7-7 .
Auto-Expand Object Groups with Prefixes	Expands object groups with the listed prefixes during the device import process. Separate the prefixes with a comma. This expansion causes the specified items to display as separate CLI during discovery. For more information, see Expanding Object Groups During Discovery, page 13-52 .
Save button	Saves your changes.

Table A-12 **Discovery Page (Continued)**

Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

IPS Updates Page

Use the IPS Updates page to perform administrative tasks associated with keeping your sensors up to date with regard to signatures, minor version updates, and service packs. You can use the IPS Updates page to:

- Monitor update status.
- Check the availability of updates and download them.
- Configure an IPS update server.
- Configure automatic update settings.



Tip

To apply IPS updates manually, select **Tools > Apply IPS Update**. For more information, see [Apply IPS Update Wizard, page A-28](#).



Caution

If you did not set Category CLI commands on your IOS IPS device to select a subset of IPS signatures that the device will attempt to compile, Security Manager will configure CLI commands to enable the IOS IPS Basic category to prevent the device resources from being overloaded. These CLI commands are not managed by Security Manager after they are deployed. You can change these manually on the device to select another set of signatures to compile.

Navigation Path

Select **Tools > Security Manager Administration** and select **IPS Updates** from the table of contents.

Related Topics

- [Configuring the IPS Update Server, page 21-9](#)
- [Checking for IPS Updates and Downloading Them, page 21-10](#)
- [Automating IPS Updates, page 21-11](#)

Field Reference

Table A-13 IPS Updates Page

Element	Description
Update Status group Refresh button	<p data-bbox="387 344 1184 375">Displays the following items. Click Refresh to update the information.</p> <ul data-bbox="400 391 1231 911" style="list-style-type: none"> <li data-bbox="400 391 1231 483">• Latest Available—The most recent signature and sensor update available on Cisco.com or the local HTTP server when you last checked for updates. <li data-bbox="400 500 1177 558">• Latest Downloaded—The most recent signature and sensor update downloaded to Security Manager. <li data-bbox="400 574 1231 633">• Latest Applied—The most recent signature and sensor update applied to any device in Security Manager. <li data-bbox="400 649 1143 708">• Latest Deployed—The most recent signature and sensor update deployed to any device in Security Manager. <li data-bbox="400 724 1231 755">• Last Check On—The time the last check of Cisco.com was performed. <li data-bbox="400 771 1163 829">• Last Download On—The time the last update was downloaded to Security Manager. <li data-bbox="400 846 1204 911">• Last Deployed On—The time the last update was deployed to any of the devices.
Check for Updates button Download Latest Updates button	<p data-bbox="387 928 1231 1084">These buttons check for updates, or download signature and sensor updates that have not already been downloaded to the Security Manager server, from the IPS Update server. You must configure an IPS Update server before checking for updates or downloading them (click Edit Settings in the Update Server group).</p> <p data-bbox="387 1101 1231 1321">When you click one of these buttons, a dialog box opens to display the results of the operation. Click Start to have Security Manager log into the IPS Update server, check for updates, and download them if you clicked the Download button. If a Cisco.com download fails, ensure that the account you are using has applied for eligibility to download strong encryption software. For details, see the description of User Name in Edit Update Server Settings Dialog Box, page A-26.</p> <p data-bbox="387 1338 1231 1432">Tip If you configure a server, and then try to check for updates, and you are told you did not configure a server, click Save at the bottom of the page and try again.</p>

Table A-13 IPS Updates Page (Continued)

Update Server group	<p>Displays the settings used to access Cisco.com or the local server that contains the IPS update packages. The fields indicate whether the update server is Cisco.com or a locally-configured HTTP server, the name of the local server if you are using one, the user account for logging into the server, and the name of the proxy server, if any. To configure or change the IPS Update server, click Edit Settings to open the Edit Update Server Settings dialog box (see Edit Update Server Settings Dialog Box, page A-26).</p> <p>For more information, see Configuring the IPS Update Server, page 21-9</p>
Auto Update Settings group	<p>Contains the settings specific to automatic updates. For more information, see Automating IPS Updates, page 21-11.</p>
Auto Update Mode	<p>Establishes whether, and to what extent, automatic updates are performed. Contains the following options:</p> <ul style="list-style-type: none"> • Download, Apply, and Deploy Updates • Disable Auto Update • Check for Updates • Download Updates • Download and Apply Updates <p>By default, auto update is disabled. The other options are a combination of one or more of the following options:</p> <ul style="list-style-type: none"> • Check for Updates—Security Manager contacts the IPS Update server to check if an update is available and sends e-mail if e-mail notification is configured. No files are downloaded. • Download Updates—Security Manager downloads the latest updates from the IPS Update server, and sends e-mail notification if e-mail notification is configured. • Apply Updates—Security Manager modifies the configuration of the devices selected in the Apply Update To list based on the downloaded update packages. You have to separately deploy these updates unless you also select Deploy Updates. • Deploy Updates—Security Manager starts a deployment job to send the applicable update packages to the devices selected in the Apply Update To list.

Table A-13 IPS Updates Page (Continued)

<p>Check for Updates</p> <p>Edit Update Schedule button</p>	<p>The schedule for the actions selected in the Auto Update Mode field. To change the schedule, click Edit Update Schedule and define the schedule in the Edit IPS Updates Schedule dialog box. You can specify that Security Manager perform the updates based on hourly, daily, weekly, or monthly schedules, or specify a one-time event. When entering the start time, use the 24-hour clock and the <i>hh:mm</i> format.</p>
<p>Notify Email</p>	<p>The e-mail address to which notifications of automatic updates are sent. If you enter more than one address, separate the addresses with commas. A notification is sent when an update:</p> <ul style="list-style-type: none"> • Is available for download. • Has been downloaded. • Has been downloaded and applied. • Has been downloaded, applied, and deployed.
<p>Apply Update To Type</p> <p>Edit Row button</p> <p>Devices to be Auto Updated</p>	<p>The selector includes the IPS devices that have local signature policies and the shared signature policies that are defined in Security Manager. The columns in the selector indicate whether a local device policy or a shared policy is selected for these types of updates:</p> <ul style="list-style-type: none"> • Signature—For auto updating the signature update level. • Minor—For minor updates and service packs. • S.P.—For service pack updates. <p>For shared policies, a partial grey checked box indicates that some, but not all, of the devices that use the policy are selected.</p> <p>Use the Type field to toggle between viewing local and shared policies. Changing the view does not change your auto update selections.</p> <p>To select a local or shared policy for auto update, select it in the selector and click the Edit Row button below the selector. This opens the Edit Auto Update Settings dialog box, where you can select the types of updates for the policy. When you select any type of auto update for a policy, the affected devices are listed in the Devices to be Auto Updated list to the right of the selector.</p>
<p>Save button</p>	<p>Saves your changes.</p>

Table A-13 *IPS Updates Page (Continued)*

Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

Edit Update Server Settings Dialog Box

Use the Edit Update Server Settings dialog box to configure the server to use for obtaining IPS updates. If necessary, you can configure a proxy server for communicating with the update server.

Navigation Path

Select **Tools > Security Manager Administration > IPS Updates** and click **Edit Settings** in the Update Server group.

Field Reference

Table A-14 *Edit Update Server Settings Dialog Box*

Element	Description
Update From	Whether to get IPS updates from Cisco.com or from a local HTTP server. Your selection changes the fields on the dialog box. If you select local, you must configure an HTTP server to use as the IPS update server.
IP Address/ Host Name (Local server only)	The host name or IP address of the local IPS update web server.
Web Server Port (Local server only)	The port number that your local server listens to for connection requests. The default is 80.

Table A-14 Edit Update Server Settings Dialog Box (Continued)

User Name	<p>The user name to log into the IPS update server. If you are configuring a local server that does not require a user login, leave this field blank.</p> <p>If you are specifying a Cisco.com user name, the user account on Cisco.com must be eligible for downloading strong encryption software. If you are not certain that the account has the required permissions, use the account to log into Cisco.com and try to download an IPS update file (http://www.cisco.com/cgi-bin/tablebuild.pl/ips5-system). If the account does not have the appropriate permissions, you are prompted to read and accept the required conditions. If you meet the eligibility requirements, you can accept them. Otherwise, talk to your Cisco sales representative for help.</p>
Password Confirm	<p>The password for the specified user name, entered in both fields. If you are configuring a local server that does not require a password, leave these fields blank.</p>
Path to Update Files (Local server only.)	<p>The path to the IPS update files location on your local server. For example, if update files can be accessed at <code>http://local-server-ip:port/update_files_path/</code>, then enter <code>update_files_path</code> in this field.</p>
Connect Using HTTPS (Local server only.)	<p>Whether to use SSL when connecting to the local IPS Update server.</p>
Proxy Server Group	
Enable Proxy Server	<p>Whether a proxy server is needed to connect to Cisco.com or to your local server.</p>
IP Address/ Host Name	<p>The hostname or IP address of the proxy server.</p>
Web Server Port	<p>The port number that the proxy server listens to for connection requests. The default is 80.</p>
User Name	<p>The user name to log into the proxy server. If the proxy server does not require a user login, leave this field blank.</p>
Password Confirm	<p>The password for the specified user name, entered in both fields. If the proxy server does not require a password, leave these fields blank.</p>

Edit Auto Update Settings Dialog Box

Use the Edit Auto Update Settings dialog box to configure the automatic update options for the device or policy selected in the Apply Update To table on the IPS Updates page. For information on configuring automatic updates, see [Automating IPS Updates, page 21-11](#).

Navigation Path

Select a device or policy on in the Apply Update To table on the IPS Updates page (see [IPS Updates Page, page A-22](#)) and click the Edit Row button.

Field Reference

Table A-15 Edit Auto Update Settings Dialog Box

Element	Description
Auto Update (IPS sensors and shared policies only)	The type of sensor updates to apply to the selected devices or shared policies. You can apply both minor updates and service packs, service packs only, or select None to apply no sensor updates automatically.
Auto Update Signature Update Level	Whether to select the device or policy for automatic signature updates.

Apply IPS Update Wizard

The Apply IPS Update wizard allows you to manually apply image and signature updates to compatible IPS devices. Before you can apply updates, you must configure an IPS Update server on the IPS Updates page (select **Tools > Security Manager Administration > IPS Updates**). For information on configuring an IPS Update server, see [Configuring the IPS Update Server, page 21-9](#).



Tip

You can configure automatic IPS updates on the IPS Updates page so that you do not have to manually apply them. For more information, see [Automating IPS Updates, page 21-11](#).

When applying signature updates, the wizard displays those signatures in the update that are not configured on the target IPS devices. In this view, you can configure the new signatures before they are applied.

When applying image and signature updates, only those devices to which the updates can be applied are available for selection; any others are gray.

**Caution**

If you did not set Category CLI commands on your IOS IPS device to select a subset of IPS signatures that the device will attempt to compile, Security Manager will configure CLI commands to enable the IOS IPS Basic category to prevent the device resources from being overloaded. These CLI commands are not managed by Security Manager after they are deployed. You can change these manually on the device to select another set of signatures to compile.

The Apply IPS Update wizard consists of these pages:

- [Step 1: Select Update To Apply Page, page A-29](#)
- [Step 2: Select Policies Update Will Be Applied To Page, page A-32](#)
- [Step 3: Edit Signatures Page, page A-33](#)

Navigation Path

Select **Tools > Apply IPS Update**.

Related Topics

- [Manually Applying IPS Updates, page 21-13](#)
- [Configuring the IPS Update Server, page 21-9](#)
- [Checking for IPS Updates and Downloading Them, page 21-10](#)
- [Automating IPS Updates, page 21-11](#)

Step 1: Select Update To Apply Page

Use the Select Update to Apply page of the Apply IPS Update wizard to select the signature or sensor update you want to apply to an IPS device or shared policy.

Navigation Path

Select **Tools > Apply IPS Update**. For more information, see [Apply IPS Update Wizard, page A-28](#).

Field Reference

Table A-16 Apply IPS Updates Wizard Step 1, Select Update to Apply Page

Element	Description
Updates Downloaded	<p>A list of the signature or sensor updates available to apply to your IPS device or policy. These files have been downloaded to the Security Manager server. Use the Type field to toggle the table between these packages:</p> <ul style="list-style-type: none"> • Sensor Updates—Displays the filename, the major, minor, and service pack, and patch versions, as well as the supported engine release. You must apply all major sensor updates, however, minor updates are cumulative. • Signature Updates—Displays the filename, the signature number, and the supported engine release. Signature updates are cumulative; however, applying them as separate packages allows you to separate your work into more manageable units if you intend to tune the updates to match the specific needs of your network. <p>Select a package from the table to apply it to your devices or policies. You can select only one package.</p> <p>To update the list of available update packages, do any of the following:</p> <ul style="list-style-type: none"> • Click Download Latest Updates. • Configure automatic downloads on the IPS Updates page (select Tools > Security Manager Administration > IPS Updates). For more information, see IPS Updates Page, page A-22. • Manually download the updates to the CSCOpX\MDC\ips\updates folder in the product installation folder (typically Program Files) on the Security Manager server.
Update Details	<p>Lists the filename, description, release number, release date, file size, and required engine level for the package selected in the Updates Downloaded list.</p>

Table A-16 Apply IPS Updates Wizard Step 1, Select Update to Apply Page (Continued)

Update Status group	<p>The Update Status group displays the following items.</p> <ul style="list-style-type: none"> • Latest Available—The most recent signature and sensor update available on Cisco.com or the local HTTP server when you last checked for updates. • Latest Downloaded—The most recent signature and sensor update downloaded to Security Manager. • Latest Applied—The most recent signature and sensor update applied to any device in Security Manager. • Latest Deployed—The most recent signature and sensor update deployed to any device in Security Manager. • Last Checked On—The time the last check of Cisco.com was performed. • Last Downloaded On—The time the last update was downloaded to Security Manager. • Last Deployed On—The time the last update was deployed to any of the devices.
<p>Check for Updates button</p> <p>Download Latest Updates button</p>	<p>These buttons check for updates, or download signature and sensor updates that have not already been downloaded to the Security Manager server from the IPS Update server. You must configure an IPS Update server before checking for updates or downloading them. To configure an IPS Update server, select Tools > Security Manager Administration > IPS Updates and click Edit Settings in the Update Server group on the IPS Updates page (for more information, see IPS Updates Page, page A-22).</p> <p>When you click one of these buttons, a dialog box opens to display the results of the operation. Click Start to have Security Manager log into the IPS Update server, check for updates, and download them if you clicked the Download button. If a Cisco.com download fails, ensure that the account you are using has applied for eligibility to download strong encryption software. For details, see the description of User Name in Edit Update Server Settings Dialog Box, page A-26.</p>

Step 2: Select Policies Update Will Be Applied To Page

Use the Select Policies Update Will Be Applied To page of the Apply IPS Update wizard to select the local or shared policy to which to apply the update. When you select a policy, the devices that use the policy are selected for update.

Navigation Path

Select **Tools > Apply IPS Update**. For more information, see [Apply IPS Update Wizard, page A-28](#).

Field Reference

Table A-17 *Apply IPS Updates Wizard Step 2, Select Policies Update Will Be Applied To Page*

Element	Description
Apply Updates to	<p>The list of policies to which you can apply the update. Use the Type field to toggle between local signature policies (representing devices not assigned to any shared signature policy) and shared signature policies. You can make selections in both lists. IPS devices to which the update does not apply are gray.</p> <p>To select all applicable devices or shared policies, click Select All. To erase your selection and start over, click Deselect All. These buttons apply only to the displayed list.</p>
Devices Assigned to Selected Policies	<p>Displays a read-only list of the devices assigned to the selected local or shared signature policies. If you select a shared policy, all devices that are using the policy appear in this list, but the devices to which the update does not apply are gray.</p>
Next button	<p>If you are applying a signature update, you can click Next to view the signatures and edit or tune them before applying the update.</p>
Finish button	<p>If you are applying a sensor update, or if you do not want to edit or tune signatures, click Finish to apply the update to the selected policies.</p>

Step 3: Edit Signatures Page

Use the Edit Signatures page of the Apply IPS Update wizard to view or edit signature updates, if desired.

Navigation Path

Select **Tools > Apply IPS Update**. For more information, see [Apply IPS Update Wizard, page A-28](#).

Field Reference

Table A-18 *Apply IPS Updates Wizard Step 3, Edit Signatures Page*

Element	Description
Filter	Allows you to filter the information displayed in the table. See Filtering Tables, page 3-24 .
Signature List	<p>Displays the new and modified signatures between the signature level of the selected update and the lowest signature level among the selected devices. If the selected devices include both IPS sensors and Cisco IOS IPS devices, the signatures for these devices appear on separate tabs.</p> <p>Click the link in the ID number to read the description for the signature on Cisco.com. The Status column indicates whether the signature is new or modified (see the visual description of the icons on the wizard page).</p> <p>To edit a signature, select it in the table and click the Edit button below the table (the pencil icon). For help in understanding the signature, click Help in the dialog box that the Edit button opens.</p> <p>For details on available signature information, see Signatures Page, page N-2. In the Signature Summary Table, you can also add custom signatures and delete signatures, but you cannot do that on this page of the Apply IPS Update Wizard.</p>
Finish button	Click this button to apply the selected update to the selected devices, and to save the edited or tuned signatures, if any.

Licensing Page

Use the Licensing page to manage licenses for the Security Manager application and for IPS devices.

Navigation Path

Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

Related Topics

- [Managing Licenses, page 21-3](#)

Field Reference

Table A-19 *Licensing Page*

Element	Description
CSM tab	The license settings for the Security Manager application. For a description of the fields on this tab, see CSM Tab, Licensing Page, page A-34 .
IPS tab	The license settings for IPS devices managed by Security Manager. For a description of the fields on this tab, see IPS Tab, Licensing Page, page A-35 .

CSM Tab, Licensing Page

Use the CSM tab on the Licensing page to view the list of installed Security Manager licenses and to install new licenses.

Navigation Path

Select **Tools > Security Manager Administration**, select **Licensing** from the table of contents, and click **CSM**.

Related Topics

- [Installing Security Manager License Files, page 21-4](#)

Field Reference

Table A-20 CSM Tab, Licensing Page

Element	Description
License Information	Displays information about the license registered with the product: the edition, license type, expiration date, the number of licensed devices, the number of devices in use, and the percentage of the device count used.
Install License	The list of installed licenses with their installation dates.
Install a License button	Click this button to install a license file. The dialog box that is opened includes links to Cisco.com, where you can obtain licenses if you have not already obtained them. You must copy license files to a local drive on the Security Manager server before you can install them.

IPS Tab, Licensing Page

Use the IPS tab on the Licensing page to view the list of installed IPS device licenses, to install new or updated licenses, or to redeploy licenses. The license list shows current licenses, unlicensed devices, devices with expired licenses, and devices with invalid licenses.

Navigation Path

Select **Tools > Security Manager Administration**, select **Licensing** from the table of contents, and click **IPS**.

Related Topics

- [Updating IPS License Files, page 21-6](#)
- [Redeploying IPS License Files, page 21-7](#)
- [Automating IPS License File Updates, page 21-7](#)
- [License Update Status Details Dialog Box, page A-38](#)

Field Reference

Table A-21 IPS Tab, Licensing Page

Element	Description
IPS License Table	Displays all of the IPS devices in the device inventory and their license status. Information includes the serial number for the device, which is used to register for licenses, the license status, and the expiration date of the license. The list shows not only current licenses, but also unlicensed devices, devices with expired licenses, and devices with invalid licenses.
Update Selected via CCO button	<p>Click this button to update the license file for the selected devices by connecting to Cisco.com and retrieving a new license. When you click this button, a dialog box opens listing devices that can be updated from Cisco.com, which might not be all of the devices you selected. Click OK to perform the update. For successful updates, the updated file is automatically applied to the device.</p> <p>To successfully update the license using this method, you must have a Cisco.com support contract that includes the serial numbers of the selected devices.</p>
Redeploy Selected Licenses button	<p>Click this button to redeploy licenses to the selected devices. Redeploying licenses might be necessary when you have obtained an updated license file and it was not applied to the device successfully during an automatic update.</p> <p>When you click this button, a dialog box opens listing devices whose licenses you are redeploying. Click OK to perform the update. For successful updates, the updated file is automatically applied to the device.</p>
Update from License File button	Click this button to update licenses by selecting a license file from the Security Manager server. When you click this button, a dialog box opens where you can specify the license files. Click Browse to select the files, which must be on a local drive on the Security Manager server. When you click OK , the updated files are automatically applied to the devices.

Table A-21 **IPS Tab, Licensing Page (Continued)**

Refresh button	Click this button to refresh the data in the IPS license table.
Download and apply licenses automatically Check	<p>Whether to automatically download IPS licenses from Cisco.com and apply them to the devices. Specify how frequently Security Manager should check for new licenses in the Check field:</p> <ul style="list-style-type: none"> • Daily—Once a day at midnight • Weekly—Once a week at midnight on Sunday • Monthly—Once a month at midnight on the first day of the month. <p>To successfully configure automatic updates, you must have a Cisco.com support contract that includes the serial numbers of your IPS devices.</p>

Updating Licenses via CCO Dialog Box

Use the Update Licenses via CCO dialog box to review the IPS devices you selected to update from Cisco.com. The device list displays the IPS devices for which you can update the license from Cisco.com, which might not be all of the devices you selected.

To successfully update the license using this method, you must have a Cisco.com support contract that includes the serial numbers of the selected devices.

When you click **OK**, the License Update Status Details dialog box (see [License Update Status Details Dialog Box, page A-38](#)) opens so that you can view the status of the update task.

Navigation Path

Select one or more device on the **Tools > Security Manager Administration > Licensing > IPS** tab and click **Update Selected via CCO**.

Redeploying Licenses Dialog Box

Use the Redeploying Licenses dialog box to review the IPS devices you selected to redeploy licenses to and to start the redeployment. Before you can redeploy a license to a device, you must have already deployed the license. Security Manager uses the file already associated with the IPS device to redeploy the license.

When you click **OK**, the License Update Status Details dialog box (see [License Update Status Details Dialog Box, page A-38](#)) opens so that you can view the status of the license redeployment task.

Navigation Path

Select one or more device on the **Tools > Security Manager Administration > Licensing > IPS** tab and click **Redeploy Selected Licenses**.

Updating Licenses from File Dialog Box

Use the Updating Licenses from File dialog box to update IPS device licenses using a license file stored on a local drive on the Security Manager server. Click **Browse** to select the license file. You can select multiple license files using Ctrl+click or a range of files using Shift+click. When you have selected the license files you want to use, click **OK** to apply them to the IPS devices.

Navigation Path

Select one or more device on the **Tools > Security Manager Administration > Licensing > IPS** tab and click **Update from License File**.

License Update Status Details Dialog Box

Use the License Update Status Details dialog box to view the status of an IPS license update task. This dialog box opens whenever you start an update task from the IPS tab of the Licensing page. For more information, see [IPS Tab, Licensing Page, page A-35](#).

Field Reference

Table A-22 License Update Status Details Dialog Box

Element	Description
Progress bar	Indicates what percentage of the license update task on the current device has been completed.
Status	The current state of the update task.
Devices to be updated	The total number of devices being updated during this task.

Table A-22 License Update Status Details Dialog Box (Continued)

Devices updated successfully	The number of devices updated without errors.
Devices updated with errors	The number of devices that generated errors during the update.
Device list	The devices that are being updated, including the device name, the status of the update, and summary information about the update. Select a device to see the messages generated during the update for that device in the message list below the summary list.
Messages list	The messages generated during the license update for the selected device. Select a message to see detailed information in the fields to the right of the list.
Description	Additional information about the message selected in the message list.
Action	The steps you should take to resolve the described problem.
Abort button	Aborts the license update task.

Logs Page

Use the Logs page to configure the default settings for the audit and operations logs. The audit log keeps a record of all state changes that occur in Security Manager.

Navigation Path

Select **Tools > Security Manager Administration** and select **Logs** from the table of contents.

Related Topics

- [Audit Report Window, page E-12](#)
- [Understanding Audit Reports, page 21-15](#)
- [Generating the Audit Report, page 21-16](#)

Field Reference

Table A-23 Logs Page

Element	Description
Keep Audit Log For Purge Now button	The maximum number of days to save audit report entries before deleting them. If the number of entries in the log exceeds the number entered in the Purge Audit Log After field, old log entries might be deleted before they reach this age. If you reduce the number of days, you can click Purge Now to immediately delete the older entries.
Purge Audit Log After (entries)	The maximum number of audit report entries to save. If an entry becomes older than the number of days specified in the Keep Audit Log For field, it is deleted even if the log has fewer than the maximum number of entries.
Keep Operation Log For	The number of days that Security Manager keeps operation logs before deleting them. These logs are used for debugging purposes.
Log Level	The level of information, according to severity, that you would like collected in the operation logs. Each level collects different amounts of data. For example, the Info level yields the most data, and the Severe level collects the least.
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Policy Management Page

Use the Policy Management page to select the types of router policies you will manage in Security Manager. These selections apply only to routers. You cannot select a subset of policy types for FWSM, ASA, PIX, or IPS devices.

For example, by selecting only certain types of policies to manage in Security Manager, you can use Security Manager to manage DHCP and NAT policies on Cisco IOS routers while leaving routing protocol policies, such as EIGRP and RIP, unmanaged. These settings apply globally in Security Manager.

Unmanaged policies are removed from both Device view and Policy view. Any unmanaged policies, local or shared, are removed from the Security Manager database. The only exception is interface policies in the Router Interfaces folder, which continue to appear in the interface but are marked as read-only policies.

You cannot unmanage a policy type if you have configured and assigned policies of that type in Security Manager. You must first remove the assignments and then unassign the policy type. If the configurations defined by those policies have already been deployed, these configurations are left in place on the devices, but the policies are no longer stored in the database and they are not accessible from the Security Manager interface.

Navigation Path

Select **Tools > Security Manager Administration** and select **Policy Management** from the table of contents.

Related Topics

- [Customizing Policy Management for Routers, page 7-47](#)
- [Chapter 15, “Managing Routers”](#)
- [Chapter 7, “Managing Policies”](#)
- [Chapter 14, “Managing IPS Services”](#)
- [Managing Shared Policies in Policy View, page 7-39](#)
- [Understanding Policies, page 7-1](#)

Field Reference

Table A-24 Policy Management Page

Element	Description
Policies to Manage	Displays the router platform policies that Security Manager manages, organized by category (NAT, Router Interfaces, and Router Platform). By default, all policies are selected. Deselected router platform policies are not managed. Deselecting the check box for a group of policies deselects all policies in that group.
Save button	Saves your changes. If policies of the selected type are assigned to even one device, an error is displayed if you deselected that policy type. The error message displays the names of the policies that are assigned, the devices to which they are assigned, and the name of the user or activity associated with this action. If you get this error message, click Cancel and manually remove the assignments in Policy view or Device view, after which you can deselect that policy type and save your changes. If the activities of other users are involved, you need to have these users remove the assignments in question.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Policy Objects Page

Use the Policy Objects page to define system defaults related to policy object creation.

Navigation Path

Select **Tools > Security Manager Administration** and select **Policy Objects** from the table of contents.

Related Topics

- [Chapter 9, “Managing Objects”](#)

Field Reference

Table A-25 Policy Objects Page

Element	Description
When Redundant Objects Detected	<p>The action you want Security Manager to take when you try to create a policy object that has the same definition as an existing object:</p> <ul style="list-style-type: none"> • Ignore—You can freely create objects with identical definitions. Any conflicts are ignored by Security Manager. • Warn—Security Manager displays a warning if you attempt to create an object that is identical to an existing object. You may proceed to create the object, if you wish. • Enforce—Security Manager prevents you from creating an object that is identical to an existing object. An error message is displayed. <p>For more information, see Guidelines for Managing Objects, page 9-4.</p>
Default Source Ports	<p>The port range value that is used as the default source port range for service objects. You can choose one of the following:</p> <ul style="list-style-type: none"> • Use all ports—Includes all ports from 1 to 65535. • Use secure ports—Includes all ports from 1024 to 65535. <p>If you change the default source ports, you must manually redeploy any previously deployed devices that might be affected. These changes might not be reflected in any open activities until you refresh the data.</p> <p>For more information on objects, see Understanding Port List Objects, page 9-168.</p>
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.

Rule Expiration Page

Use the Rule Expiration page to define the default values for policy rule expiration. When you create policies for some types of policy rules (such as access rules), you can set an expiration date for the rule, and Security Manager can notify you by e-mail of the approaching expiration date.

You must configure an SMTP server to enable e-mail notifications. For more information, see [Configuring an SMTP Server and Default Addresses for E-Mail Notifications](#), page 1-18.

Navigation Path

Select **Tools > Security Manager Administration** and select **Rule Expiration** from the table of contents.

Field Reference

Table A-26 *Rule Expiration Page*

Element	Description
Notify Email	The default e-mail address that should receive notifications of rule expiration. Users can override this address when configuring individual rules.
Notify Before Expiration	The default number of days before a rule expires that Security Manager should send the e-mail message. Users can override this value when configuring individual rules.
Sender	The e-mail address that Security Manager will use for sending e-mail notifications.
Email Format	The format of the e-mail message: <ul style="list-style-type: none"> • Text—The e-mail is sent in HTML and plain text formats. • XML—The e-mail is sent using an XML markup. This option might be appropriate if you decide to write a program to automatically process and respond to notifications.
Save button	Saves your changes.
Reset button	Restores all fields to their previous values.
Restore Defaults button	Resets values to Security Manager defaults.

Server Security Page

Use the Server Security page to open specific pages in the CiscoWorks Common Services application, where you can configure various security features on the Security Manager server. CiscoWorks Common Services controls the basic functions of the Security Manager server, including user access control and system security.

When you log in to Security Manager, your user name and password are compared with the account information stored in the CiscoWorks or Cisco Secure Access Control Server (ACS) database, depending on which system you established at installation as your AAA provider. After the authentication of your credentials, you have access according to the role you have been assigned.

For more information on Security Manager roles and privileges, including descriptions of how Common Services roles translate to user functions in Security Manager, see [Setting Up User Permissions, page 2-1](#).

Navigation Path

Select **Tools > Security Manager Administration** and select **Server Security** from the table of contents.

Related Topics

- [Default Associations Between Permissions and Roles in Security Manager, page 2-31](#)
- [Understanding Cisco Secure ACS Roles, page 2-28](#)
- [Understanding CiscoWorks Roles, page 2-25](#)

Field Reference

Table A-27 Server Security Page

Element	Description
AAA Setup button	Opens Common Services and displays the AAA Mode Setup page. From this page, you can set AAA as your fallback sign-on method. For more information about AAA, click Help from the AAA Mode Setup page.
Certificate Setup button	Opens Common Services and displays the Self-Signed Certificate Setup page. CiscoWorks enables you to create self-signed security certificates, which you can use to enable SSL connections between your client browser and management server. For more information about self-signed certificates, click Help from the Certificate Setup page.
Single Sign On button	Opens Common Services and displays the Single Sign-On Setup page. With Single Sign On (SSO), you can use your browser session to transparently navigate to multiple CiscoWorks servers without having to authenticate to each of them. Communication between multiple CiscoWorks servers is enabled by a trust mode addressed by certificates and shared secrets. For more information about setting up SSO, click Help from the Single Sign-On page.
Local User Setup	Opens Common Services and displays the Local User Setup page, from which you can add and delete users, edit user settings, and assign roles or permissions. For more information, click Help from the Local User Setup page and see Default Associations Between Permissions and Roles in Security Manager, page 2-31 .
System Identity Setup	Opens Common Services and displays the System Identity Setup page. Communication between multiple CiscoWorks servers is enabled by a trust mode addressed by certificates and shared secrets. System Identity setup helps you to create a trust user on servers that are part of a multi-server setup. For more information about system identity setup, click Help from the System Identity Setup page.

Status Page

Use the Status page to select the providers that will provide status to users when they view their inventory status by selecting **Tools > Inventory Status**. The status is displayed on the Status tab in the Inventory Status window.

By default, Security Manager provides status on deployment to the devices, but you can add Performance Monitor servers if you use them to monitor your network.

Navigation Path

Select **Tools > Security Manager Administration** and select **Status** from the table of contents.

Related Topics

- [Configuring Status Providers, page 1-24](#)
- [Inventory Status Window, page C-49](#)
- [Viewing Inventory Status, page 6-30](#)

Field Reference

Table A-28 **Status Page**

Element	Description
Connect Devices Status	
Deployment	Whether to include the status of deployment jobs that include the device.
Providers table	
The providers table lists the Performance Monitor servers that are registered with Security Manager. You can add up to five servers.	
Provider	The name of the Performance Monitor server. This name appears in the Inventory Status window on the Status tab for individual devices, indicating the server that provided the status.
Short name	The nickname for the provider name.
Status	Whether Security Manager should actively poll the Performance Monitor server for status. Select Enabled to actively poll the server, or Disabled to suspend polling the server without having to delete the provider entry.

Table A-28 **Status Page (Continued)**

Add button (+ icon)	Click this button to add a provider to the list. The Add Status Provider dialog box opens (see Add or Edit Status Provider Dialog Box, page A-48).
Edit button (pencil icon)	Click this button to edit the properties of the selected provider. The Edit Status Provider dialog box opens (see Add or Edit Status Provider Dialog Box, page A-48).
Trash button (trash can icon)	Click this button to delete the selected provider.
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.

Add or Edit Status Provider Dialog Box

Use the Add or Edit Status Provider dialog box to register a Performance Monitor server with Security Manager. Security Manager can then poll the Performance Monitor servers for event status such as VPN tunnels, device connectivity, and CPU usage threshold. Users can view the status of their devices by selecting **Tools > Inventory Status**.

Navigation Path

To open this dialog box, select **Tools > Security Manager Administration**, then click **Status** to open the Status page. Then, do one of the following:

- Click the Add button to register a new server.
- Select an existing server and click the Edit button to edit the server properties.

Related Topics

- [Configuring Status Providers, page 1-24](#)
- [Inventory Status Window, page C-49](#)
- [Status Page, page A-47](#)
- [Viewing Inventory Status, page 6-30](#)

Field Reference

Table A-29 Add or Edit Status Provider Dialog Box

Element	Description
Provider name	The name of the service provider, for example, Performance Monitor. You can enter up to 128 characters. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: - _ :. and space.
Server	The IP address or fully-qualified host name of the Performance Monitor server. The host name can be up to 128 characters.
Short Name	The short name for the provider name.
Port	The port number that Security Manager should use to communicate with the Performance Monitor server. The default is 443.
Poll Cycle	The number of minutes the firewall device will wait between polling Performance Monitor for new information. The default is 600 seconds (10 minutes). The minimum time is 60 seconds.
Username	The username for logging in to Performance Monitor.
Password	The password for logging in to Performance Monitor. In the Confirm field, enter the password again.
URN	<p>The uniform resource name for Performance Monitor. URN is the name that identifies the resource on the Internet. URN is part of a URL, for example, /mcp/StatusServlet. The full URL could be:</p> <p><code>https://:<server ip> :443/mcp/StatusServlet</code></p> <p>where:</p> <ul style="list-style-type: none"> • <server ip> is the IP address of Performance Monitor. • 443 is the port number Performance Monitor listens to. • /mcp/StatusServlet is the URN of the Performance Monitor.
Status	Whether the server is enabled for providing status to Security Manager. If you select Disabled, the server is added to the status providers list, but Security Manager does not poll it for status.

Take Over User Session Page

Use the Take Over User Session page to take over another user's configuration session. A user with administrative privileges can take over the work of another user in non-Workflow mode. Taking over a session is useful when a user is working on devices and policies, causing the devices and policies to be locked, and another user needs access to the same devices and policies.

Navigation Path

Select **Tools > Security Manager Administration** and select **Take Over User Session** from the table of contents.

Related Topics

- [Taking Over Another User's Work, page 21-17](#)

Field Reference

Table A-30 *Take Over User Session Page*

Element	Description
User	The user name of the person who's session you might take over.
Session State	The state of the session, whether the user is currently logged in or logged out.
Take over session button	Click this button to take over the selected configuration session, transferring the changes made by the selected user to the currently logged in user. Any changes that have not already been committed are discarded. If the selected user is logged in at the time changes are taken over, the user receives a warning message, loses the changes in progress, and then is logged out.

Token Management Page

Use the Token Management page to identify the Token Management Server (TMS) to use for deploying configurations to Cisco IOS routers that use TMS as the communication protocol. Security Manager uses the settings on this page to contact the TMS server.

Security Manager uses FTP to deploy the configuration file to the TMS server, from which the configuration file can be downloaded and encrypted onto an eToken.

To use TMS with Cisco IOS routers, you must specify TMS as the transport protocol. You can do this for all routers on the Device Communication page (see [Device Communication Page, page A-14](#)), or for a specific router in its device properties (see [General Page, page C-36](#)). You must also configure the TMS server as an FTP server, otherwise deployment will fail.

Navigation Path

Select **Tools > Security Manager Administration** and select **Token Management** from the table of contents.

Related Topics

- [Frequently Asked Questions about Deployment, page 19-17](#)
- [Setting Up TMS, page 5-22](#)
- [Understanding Deployment Methods, page 19-11](#)

Field Reference

Table A-31 **Token Management Page**

Element	Description
Server Name or IP Address	The DNS hostname or IP address of the TMS server.
Username	The username Security Manager should use to log on to the TMS server.
Password	The password for the username. Enter the password in both fields.
Confirm Password	

Table A-31 Token Management Page (Continued)

Directory in the TMS Server for Config Files	The directory on the TMS server where deployed configuration files will be downloaded. The root FTP directory (“.”) is the default FTP location on the TMS server.
Public Key File Location	The location of the public and private key files on the Security Manager server, as copied from the TMS server. Security Manager uses the public key to encrypt data sent to the TMS server. Then the server uses its private key to decrypt the data. Security Manager comes with a default public key that matches the default private key on the server. Note If needed, you can generate a new pair of public and private keys using the TMS server. If you do this, you need to copy the new public key to the Security Manager server.
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets values to Security Manager defaults.

VPN Policy Defaults Page

Use the VPN Policy Defaults page to view or assign the default VPN policies that Security Manager uses for each IPsec technology. To select a policy as a default policy, you must create it as a shared policy.

Security Manager uses VPN policy defaults to simplify VPN configuration while ensuring that policy consistency is maintained. Security Manager provides mandatory policies as factory defaults, which means they are configured on the devices in your VPN topology with predefined values, depending on the assigned IPsec technology. Factory default policies with their default configurations enable you to deploy to your devices immediately after creating the VPN topology. Factory default policies are private policies and are not viewable. Optional policies are not provided as factory defaults.

The VPN Policy Defaults page has eight tabbed areas. Six of these tabs are for the following VPN technologies:

- DMVPN
- Large Scale DMVPN
- Easy VPN

- IPsec/GRE
- GRE Dynamic IP
- Regular IPsec

The other two tabs cover default settings for S2S (site-to-site) Endpoints and Remote Access.

Navigation Path

Select **Tools > Security Manager Administration** and select **VPN Policy Defaults** from the table of contents.

Related Topics

- [Understanding VPN Default Policies, page 10-11](#)
- [Assigning Default Policies to Your VPN Topology, page 10-30](#)
- [Assigning the Default Remote Access VPN Policies, page 11-11](#)

Field Reference

Table A-32 *VPN Policy Defaults Page*

Element	Description
DMVPN tab	Lists the six policy types for the Dynamic Multipoint VPN technology, and shows the name of the current default policy for each policy type. The types include the following: <ul style="list-style-type: none"> • GRE (DMVPN) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings

Table A-32 VPN Policy Defaults Page (Continued)

Large Scale DMVPN tab	<p>Lists the six policy types for the Large Scale Dynamic Multipoint VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • GRE (Large Scale) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings
Easy VPN tab	<p>Lists the seven policy types for the Easy VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • Client Connection Characteristics • Easy VPN IPsec Proposal • IKE Proposal • PIX7.0/ASA Tunnel Group Policy • Public Key Infrastructure • User Group Policy • VPN Global Settings
IPsec/GRE tab	<p>Lists the six policy types for the IPsec/GRE VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • GRE (GRE Method) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings

Table A-32 **VPN Policy Defaults Page (Continued)**

GRE Dynamic IP tab	<p>Lists the six policy types for the IPsec/GRE VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • GRE (Dynamic IP) • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings
Regular IPsec tab	<p>Lists the five policy types for regular IPsec VPN technology, and shows the name of the current default policy for each policy type. The types include the following:</p> <ul style="list-style-type: none"> • IKE Proposal • IPsec Proposal • Preshared Key • Public Key Infrastructure • VPN Global Settings
S2S Endpoints tab	<p>Presents drop-down lists for Internal and External endpoints, each of which you can configure to:</p> <ul style="list-style-type: none"> • All Interfaces • Internal • External
(Policy Type Drop Down List)	<p>Lists the policies that are available to be set as the default policy for each policy type. Until you create shared VPN policies, only Factory Default is listed.</p>

Table A-32 VPN Policy Defaults Page (Continued)

View Content	<p>Opens the detailed specification page for each VPN policy. Although you can change the contents of the fields in the specification page, you cannot save your changes; the displayed information is read-only.</p> <p>Note Some policy types have empty factory defaults. When you try to view content of an empty policy type you receive the following message: <i>Info- There are no policy defaults for this policy type.</i></p>
Save button	Saves your changes.
Reset button	Resets changes to the last saved values.
Restore Defaults button	Resets all policy values to Security Manager defaults.

Workflow Page

Use the Workflow page to select the workflow mode that Security Manager enforces and to define the default settings for activity and deployment job notifications and logging.

Before changing the workflow mode, read the following topics to understand how the modes differ and the effects of changing the modes:

- [Working in Workflow Mode, page 1-20](#)
- [Working in Non-Workflow Mode, page 1-21](#)
- [Comparing the Two Workflow Modes, page 1-21](#)
- [Changing Workflow Modes, page 1-23](#)

Navigation Path

Click **Tools > Security Manager Administration** and select **Workflow** from the table of contents.

Related Topics

- [Chapter 8, “Managing Activities”](#)
- [Chapter 19, “Managing Deployment”](#)

Field Reference

Table A-33 Workflow Page

Element	Description
Workflow Control	
Enable Workflow	Whether to enable Workflow mode. When Workflow mode is enabled, you can select whether to have an approver for activities and deployment jobs.
Require Activity Approval	Whether to require that activities be approved explicitly by an assigned approver. For more information about the differences between working with and without an approver, see Activity Approval, page 8-3 .
Require Deployment Approval	Whether to require that deployment jobs be approved explicitly by an assigned approver. For more information about the differences between working with and without an approver, see Understanding Deployment, page 19-1 .
Email Notifications	
Sender	The e-mail address that Security Manager will use for sending e-mail notifications.
Activity Approver	The default e-mail address for the person responsible for approving activities. Users can override this address when submitting an activity for approval. For more information, see Submitting an Activity for Approval, page 8-18 .
Job/Schedule Approver	The default e-mail address of the person responsible for approving deployment jobs or schedules. Users can override this address when submitting a job or schedule for approval. For more information, see Submitting Deployment Jobs, page 19-39 .
Job Completion Notification	The e-mail address of the person who should receive notification when deployment jobs are completed. Users can override this address when creating a deployment job.
Include Job Deployer	Whether to send notifications of deployment job status changes to the person who deployed the job.
Require Deployment Status Notification	Whether to have e-mail notifications sent whenever the status of a deployment job changes.

Table A-33 Workflow Page (Continued)

Workflow History	
Keep Activity for	<p>The number of days that activity information should be kept in the Activity table. The default is 30. You can specify from 1 to 180 days.</p> <p>Click Purge Now to delete all activities older than the number of days specified.</p>
Keep Job for	<p>The number of days that deployment job information should be kept in the Deployment Job table. The default is 30. You can specify from 1 to 180 days.</p> <p>Click Purge Now to delete all jobs older than the number of days specified.</p>
Keep job per schedule for	<p>The number of days that deployment job information should be kept in the Deployment Job table for each job schedule. This setting applies only to jobs that were initiated by a schedule. The default is 30. You can specify from 1 to 180 days.</p> <p>Click Purge Now to delete all jobs older than the number of days specified.</p>
Save button	Saves your changes.
Reset button	Resets changes to the previously applied values.
Restore Defaults button	Resets values to Security Manager defaults.